What is claimed is:

1. A method for provisioning and registering a packet-switched communications device in an enterprise network, comprising:

providing an unprovisioned packet-switched communications device in an enterprise network, the packet-switched communications device having a corresponding unique identifier;

as part of the provisioning process establishing a secure communications session with a key generating agent in the enterprise network;

providing, to the key generating agent through the session, i) the unique identifier associated with the communications device when a key identifier is derived using the unique identifier or ii) no unique identifier when the key identifier is derived using information not associated with the communications device;

receiving, from the key generating agent through the session, a secret key derived from the key identifier;

forwarding to an application server a registration request, wherein the registration request comprising the key identifier;

authenticating the communications device with the secret key; and

when the communications device is successfully authenticated, registering the communications device.

2. The method of Claim 1, wherein the key identifier is a function of at least one of a psuedo-random number generator, a database of keys and key identifiers, and a hash function.

3. The method of Claim 1, wherein the communications device possesses a secret key and the communications device is not in secure communications with the application server, wherein the communications device provides a registration request to the application server using the key identifier.

4. The method of Claim 1, further comprising before the establishing step:

authenticating the key generating agent;

performing the establishing, providing, and receiving steps when authenticating the key generating agent is successful.

5. The method of Claim 1, wherein the secret key is a symmetric key.

6. The method of Claim 1, wherein the secret key is derived from an enterprise master key.

7. The method of Claim 6, wherein the enterprise master key is calculated using a seed value and a pseudorandom number generator.

8. The method of Claim 1, wherein the secret key is derived from an enterprise master key and the key identifier.

9. The method of Claim 1, wherein the key identifier computed from a unique identifier comprises at least a first field, the first field comprising an identifier

associated with the key generating agent, a second field comprising the identifier of the communications device, and a counter field.

10. The method of Claim 9, wherein the unique identifier of the communications device is at least one of an extension on the enterprise network, a serial number, a user login identifier, and an address of the communications device on the enterprise network.

11. The method of Claim 1, further comprising:

digitally signing a message, wherein the digital signature is derived from the secret key, a constant, and the personal identification number of a user associated with the communications device.

12. The method of Claim 1, wherein the receiving step further comprises receiving, from the key generating agent through the session, a key identifier.

13. The method of Claim 1, further comprising before the establishing step:

receiving an IP address assigned to the communications device.

14. The method of Claim 1, wherein the establishing step comprises:

establishing a logical connection with the key generating agent;

negotiating security parameters;

authenticating the identity of the key generating agent; and

when authentication is successful, activating the negotiated security parameters to establish the secured communications session.

15. The method of Claim 4, further comprising:

when authentication is successful, establishing secure communications.

16. The method of Claim 1, wherein the providing step comprises prompting a user associated with the communications device for a personal identification number and unique identifier.

17. The method of Claim 1, wherein the communications device provides to the key generating agent through the session, the key identifier when the communications device computes the key identifier.

18. The method of Claim 1, further comprising:

closing the secured session; and

computing a packet switched device authentication key using the secret key.

19. The method of Claim 1, wherein the step of authenticating further comprising:

when authentication is successful, establishing secure communication with the communications device.

20. A computer readable medium comprising instructions to perform the steps of Claim 1.

21. The method of Claim 1, wherein the establishing, providing and receiving steps are free of a challenge message and a response thereto.

22. A logic circuit operable to perform the steps of Claim 1.

23. A packet-switched communications device in an enterprise network, the packet-switched communications device having a corresponding unique identifier, comprising:

a processor in the packet-switched communications device operable to:

(a) establish a secure communications session with a key generating agent in the enterprise network;

(b) provide, to the key generating agent through the session, i) the unique identifier associated with the communications device when a key identifier is derived using the unique identifier or ii) no unique identifier when the key identifier is derived using information not associated with the communications device; and

(c) receive, from the key generating agent through the session, a secret key and a key identifier;

(d) forward to an application server a registration request, wherein the registration request comprises the key identifier and the application server further comprising a second processor that is operable to:

authenticate the communications device with the secret key; and

when the communications device is successfully authenticated, register the communications device.

24. The packet-switched communications device of Claim 23, wherein the packet-switched communications device is unprovisioned and does not possess the secret key before the receiving function.

25. The packet-switched communications device of Claim 23, wherein the key identifier is a function of at least one of a psuedo-random number generator, a database of keys and key identifiers, and a hash function.

26. The packet-switched communications device of Claim 23, wherein the communications device processor is further operable, before the establishing function, to:

authenticate the key generating agent; and

perform the establishing, providing, and receiving functions when authentication of the key generating agent is successful.

27. The packet-switched communications device of Claim 23, wherein the secret key is a symmetric key.

28. The packet-switched communications device of Claim 23, wherein the secret key is derived from an enterprise master key.

29. The packet-switched communications device of Claim 28, wherein the enterprise master key is calculated using a seed value and a pseudorandom number generator based on a secure hash algorithm.

30. The packet-switched communications device of Claim 28, wherein the secret key is derived from the enterprise master key and the key identifier.

31. The packet-switched communications device of Claim 23, wherein the key identifier comprises at least a first field, the first field comprising an identifier associated with the key generating agent, a second field comprising the identifier of the communications device, and a counter field.

32. The packet-switched communications device of Claim 31, wherein the unique identifier of the communications device is at least one of an extension on the enterprise network, a serial number, a user login identifier, and an address of the communications device on the enterprise network.

33. The packet-switched communications device of Claim 23, wherein the processor is further operable to:

digitally sign a message, wherein the digital signature is derived from the secret key, a constant, and the personal identification number of a user associated with the communications device.

34. The packet-switched communications device of Claim 23, wherein the communications device possesses a secret key and the communications device is not in secure communications with the application server of the enterprise network, wherein the communications device provides a registration request to the application server using the key identifier.

35. The packet-switched communications device of Claim 23, wherein the processor is further operable, before performing the establishing function, to:

receive an IP address assigned to the communications device.

36. The packet-switched communications device of Claim 23, wherein the establishing function comprises the operations of:

establishing a logical connection with the key generating agent;

negotiating security parameters;

authenticating the identity of the key generating agent; and

after authentication is successful, activating the negotiated security parameters to establish the secured communications session.

37. The packet-switched communications device of Claim 26, wherein the processor is further operable to:

when authentication is successful, establish secure communication.

38. The packet-switched communications device of Claim 23, wherein the providing function comprises prompting a user associated with the communications device for a personal identification number and the unique identifier.

39. The packet-switched communications device of Claim 23, wherein the receiving function comprising the operation of:

generating the secret key using the key identifier and the enterprise master key.

40. The packet-switched communications device of Claim 23, wherein the processor is further operable to:

close the secured session and

compute a packet switched device authentication key using the secret key.

41. The packet-switched communications device of Claim 23, wherein the second processor is further operable, when authentication is successful establish secure communication with the communications device.

42. The packet-switched communications device of Claim 23, wherein the establishing, providing and receiving functions are free of a challenge message transmitted to the communications device and/or to the key generating agent.

43. A method for provisioning and registering a packet-switched communications device in an enterprise network, comprising:

assigning an electronic address to the communications device;

providing the electronic address and an address associated with a key generating agent to the communications device;

communications device authenticating the key generating agent; and

when authentication of the key generating agent is successful, performing the following functions:

establishing a secure communications session with the key generating agent;

generating a secret key i) using the unique identifier of the communications device when a key identifier is derived using the unique identifier or ii) not using the unique identifier when the key identifier is derived using information not associated with the communications device; and

providing, to the communications device through the session, the secret key;

an application server receiving a registration request from the communications device, wherein the registration request comprises the key identifier ;

the application server authenticating the communications device using the secret key; and

when the communications device is successfully authenticated, registering the communications device.

44. The method of Claim 43, wherein the packet-switched communications device is not yet provisioned in the establishing, generating, and providing steps, wherein the packet-switched communications device does not yet possess the secret key before the providing step, and wherein, in the providing step, the key generating agent also provides a key identifier.

45. The method of Claim 44, wherein the key identifier is a function of at least one of a psuedo-random number generator, a database of keys and key identifiers, and a hash function.

46. The method of Claim 43, wherein the secret key is a symmetric key.

47. The method of Claim 44, wherein the secret key is derived from an enterprise master key.

48. The method of Claim 47, wherein the enterprise master key is calculated using a seed value and a pseudorandom number generator based on a secure hash algorithm.

49. The method of Claim 47, wherein the secret key is derived from the enterprise master key and the key identifier.

50. The method of Claim 44, wherein the key identifier comprises at least a first field, the first field comprising an identifier associated with the key generating agent, a second field comprising the identifier of the communications device, and a counter field.

51. The method of Claim 50, wherein the unique identifier of the communications device is at least one of an extension on the enterprise network, a serial number, a user login identifier, and an address of the communications device on the enterprise network.

52. The method of Claim 43, further comprising:

digitally signing a message, wherein the digital signature is derived from the secret key, a constant, and the personal identification number of a user associated with the communications device.

53. The method of Claim 43, wherein the communications device possesses a secret key and the communications device is not in secure communications with an application server of the enterprise network, wherein the communications device provides a registration request to the application server using the key identifier.

54. The method of Claim 43, wherein the establishing step comprises:

establishing a logical connection with the communications device;

negotiating security parameters;

authenticating the identity of the key generating agent; and after authentication is successful, activating the negotiated security parameters to establish the secured communications session.

55. The method of Claim 43, wherein the providing step further comprising:

providing, to the communications device through the session, the key identifier.

56. The method of Claim 43, further comprising:

closing the secured session; and

computing a packet switched device authentication key using the secret key.

57. The method of Claim 43, wherein the step of authenticating the communications device further comprising:

when authentication is successful, establishing secure communications.

58. A computer readable medium comprising instructions to perform the steps of Claim 43.

59. A logic circuit operable to perform the steps of Claim 43.

60. A method for registering a communications device in an enterprise network comprising:

providing to an application server, a request for registration from the communications device including a key identifier;

establishing a communication connection between the application server and a key generating agent;

transmitting a request from the application server to the key generating agent for a secret key corresponding to the key identifier;

sending the secret key derived for the key identifier to the application server;

the application server authenticating the communications device; and

the application server registering the communications device after a successful authentication.

61. The method of claim 60, wherein the establishing step further comprises:

establishing a logical connection between the application server and the key generating agent;

negotiating security parameters;

mutually authenticating the key generating agent and the application server; and

establishing secure communications.

62. The method of claim 60, wherein the step of authenticating the communications device further comprising: authenticating the communications device with the secret key associated with the key identifier and when authentication is successful, establishing secure communications.